CYBER SECURITY

INCIDENT RESPONSE

PLAN

ISSUE 1

CONTENTS

APPENDICES

Circulation List

Name	Title
	CEO
	CFO
	Vice President of Extrusion Division
	Vice President of Vascular Division
	Vice President of Molding Division
	Vice President of IT
	Vice President of Human Resources
	VP/Corporate Controller
	Human Resources Director
	IT Operations Manager

1 Introduction

This Cyber Security Incident Response Plan ("the Plan") has been compiled with the objective of creating a plan for Spectrum Plastics Group ("the Company") to follow in the event of a cyber security incident.

The nature of any incident and the severity of the restrictions it places on the Company's operation cannot be known in advance.

Rapid assessment of the situation and the taking of appropriate contingency action are vital to limit disruption in the interests of both the Company and its customers.

2 Initial Response to an Incident

An Incident Team will be formed to coordinate the response to any incident. The Team will be made up of (as required).

	CEO
	CFO
	Vice President of Medical Tubing Division
	Vice President of Vascular Division
	Vice President of Molding Division
	Vice President of IT
	Vice President of Human Resources
	VP/Corporate Controller
	Human Resources Director
	IT Operations Manager

If the incident occurs during a workday, the Incident Team shall assemble in the Main Conference Room. Team members who are absent should be contacted, if necessary. Home and cell phone numbers of team members are listed in Appendix I. If the incident occurs outside normal business hours, the team will convene via conference call.

If the incident occurs at night, the VP of IT should contact the CFO at the first instance, followed by the CEO and the VP of Human Resources.

The initial role of the Incident Team shall be as follows:

- Determine the extent of the incident.
- Launch an investigation into the cause of the incident.
- Contact VP/Corporate Controller to alert the insurers.

- Determine the best means of communication (cell phones, faxes, etc).
- Activate the IT Disaster Recovery procedure if necessary (see Appendix II).
- Assess the expected time lapse prior to restoring the ability of the Company to do business (completely or partially).

Based on the above action and information, the Incident Team can start to assess the impact of the cyber incident and to start a plan of action to meet the Company's needs.

3 The Assessment Process

As each potential cyber incident is different, not all items listed below will be relevant to each incident. However, the Incident Team should use the following guidelines to assist in its decision-making process:

3.1 Phishing Attack (Personal Information):

- What information has been leaked?
  - Is it Employee Information?
    - Is it Personal Identifiable Information? (PII)
  - Is it customer information?
- Is access affected? If so, how soon will it be free?

3.2 Malware, Cryptolocker, Virus Attack:

- What sites are affected?
- Can the site connect to the internet?
- Has production/operation been affected?
- What systems are affected?
- Which servers have been rendered unusable?
- Which programs have been rendered unusable?
- How soon will they be restored to partial/full use?

4 The Contingency Plan

If the assessment of the incident reveals that the Company cannot meet the requirements of their respective employees, users, or customers, the following action should be considered by the Incident Team:

- Contact Legal Representatives of the Company
- Prepare drafts for discussions with affected users or customers which could include:
  - explanation of situation;
  - explanation of next steps
- Keep employees informed of events and, if they are sent home for a period due to lack of work, check that contact numbers are available and current.

- Contact third-party IT firms for the connected plants;

If production is affected:

- In discussion with the CEO/VP of the Division of Spectrum (SPG) determine which items can be manufactured/shipped from other plants within the group;
- Contact customers to discuss alternative arrangements;
- Prioritise customer orders and inform customers of any revision to delivery date;
- Keep customers informed of progress;

5 The Restoration Plan

The Incident Team should also begin work as soon as possible toward organizing the restoration of systems to full operational status or the employee(s) data, depending on the incident. Action which might be necessary, depending on the incident, includes:

- Provide guidance for plans of action and precautions to be taken during the forensic report.
- Order replacement IT hardware and software in preparation for termination of IT disaster recovery service (as outlined in Appendix II).
- Contract with third party identity theft protection service to provide credit and identity monitoring services to employees.
- Post mortem analysis
- Training and stop-gap analysis

6 Other Issues

6.1 Continual Review of Situation

It is vital that the Incident Team be kept informed of all developments. Employees involved in both the Contingency and Restoration Plans must have full knowledge of all developments when they are asked to carry out any tasks. The Incident Team should meet at least once a day (timing to be agreed upon) to ensure that all members are informed of the latest developments and actions.

6.2 Insurance

Details of all costs and losses incurred because of the incident should be recorded and forwarded to the CFO of Spectrum (SPG).

APPENDIX I

Cyber Security Incident Team – Contact Numbers

Name	Cell Telephone Number

APPENDIX II

IT Disaster Recovery Procedure

- The Spectrum (SPG) Atlanta IT Department provides coverage 24 hours all business days.
- Emergency contact numbers for all IT personnel:

Name	Telephone Number

- The local IT Systems are backed up locally and then sent off site to the Co-location facility. All backups are able to spin up on backup hardware so limited outages should occur.
- Useful contact numbers for technical support:

For	Contact	Telephone No. *Email (if applicable)*
Telephone System		
Telephones/PBX		
IFS Software		
Internet Provision		
T-1 Lines		
Computers (New PC's)		
PC Supplies		
PC/Servers		
Sites		

APPENDIX III

Details of Spectrum (SPG), LLC Facilities

Facility	Telephone No	Fax No