Incident Response Policy

Goals

- Ensure the StaffCircle responds to an IT breach or cyber-attack in an appropriate and consistent matter.
- To ensure we have a framework and policy which can provide ongoing improvements to our response and the security of our ongoing service.

Scope

This document has been created in accordance with the National Cyber Security Centre and ICO and covers potential IT breach or cyber-attack scenarios that may affect the usage, loss or theft of data contained within the StaffCircle Platform as of 20 November 2020. This focuses on the procedural elements of our policy in response to the outlined scenarios.

Key Contacts

The following contacts should be available to respond to either a IT Breach or Cyber-Attack.

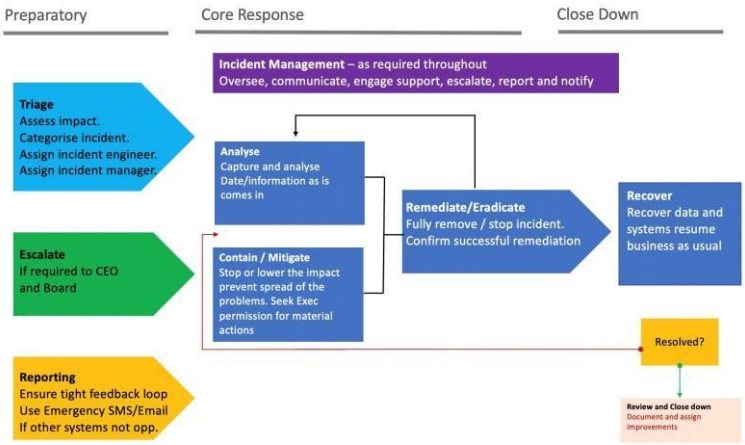
Response Teams Key Contacts					
Name	Role	Response	Email	Telephone	Response Time
Chris keeber	Security Lead & DPO	Primary Contact	incident@staffcircle.com	01162183330	2 Hours
Ben Barker	VP Product	Secondary Contact	incident@staffcircle.com	01162183330	2 Hours
Mark Seemann	CEO	Escalatory Contact	Mark.seemann@staffcircle.com	01162183330	5 hours

Escalation Criteria

Initially if being reported by a customer, an incident report should be emailed to incident@staffcircle.com or customer support on 01162183330

If the response time has elapsed (total 4 hours) then email mark.seemann@staffcircle.com In either case, the ICO will be notified of any data breach within 72 hours of the discovery of a data breach.

Basic Flowchart of Process



All external facing APIs and UX are measured in real-time by our customer facing status engine which

is available at

https://status.staffcircle.com