**A.4 APPENDIX 7**

# DIGITAL CYBER INCIDENT RESPONSE PLAN (CIRP)

Issued by: Head of Digital & Assurance Services

Version: 1.0 September 2022

Agreed By Management Team 27 September 2022

Agreed By Member Task & Finish Cyber-Security Group 8th December 2022

## Table of Contents

## 1. PURPOSE:

The purpose of this digital services (IT) continuity and disaster recovery plan is to document the governance, planning and procedures that will be followed during a cyber-attack incident response and recovery scenario.

This plan definitively outlines how Tendring District Council will respond when a cyber-attack occurs.

## 2. DIGITAL SERVICE RECOVERY SCOPE

The scope of this recovery plan is limited to;

- All core digital infrastructure - hardware and applications software - managed by the council's digital service and incumbent network management partners (currently Intergence Systems Ltd).

- All critical systems (software applications) managed by the council's digital service - both on-premise and cloud-based.

- All non-critical systems managed (as above).

Council departments have out-sourced some specialist applications to third parties with whom they have a managed service contract. These out-sourced digital services are specifically out-of-scope of this continuity and recovery plan as we are reliant upon their contractual recovery response management.

However, the council's Digital Services and Assurance Team will provide technical advice and guidance to council service-sponsors, subject to resource availability and any situation associated resource prioritisation.

## 3. BACKGROUND AND BUSINESS CONTINUITY OBJECTIVES

Tendring District Council seeks to provide high quality, affordable digital services that are accessible, easy to use and highly resilient for service users – residents, customers, visitors, members and officers alike.

As best practice, our Cyber Incident Planning and Response (CIPR) certificated training strongly advocates that an organisation should document, update and exercise a Cyber Incident Response Plan (CIRP) that is adopted by its management group and accords with the organisations business continuity and recovery priority goals. This ethos is echoed by the Local Government Association.

Response/ recovery incident post-situational learning taught us that 'seasoned' IT staff were 'confident' with managing and resolving a cyber-attack response. However, for newer management and operational staff this was their very first cyber-attack situation and were keen to play their part but needed close direction and guidance. This identified the need for a document to refer to and the need to exercise and train newer staff.

Similarly, as a response becomes prolonged/ intensified and with key staff working extended hours over a number of days - stress, leadership and management fatigue and self-doubts will occur. Again, as a lesson learnt, the need for a documented/ adopted CIRP as a reference guide will aid and boosted flagging confidence levels.

This digital services Cyber Incident Response Plan (CIRP) covers the widest possible range of scenarios, addressing risks such as: network connectivity failure, failure/ destruction of hardware, data corruption, phishing, smishing, fraud, ransomware cyberattack(s).

Again, following best practice, the council’s CIRP is based upon National Institute of Standards and Technology (NIST) cyber-attack response standards (as adopted by the National Cyber Security Centre [NCSC]), this CIRP follows the 4 cyber incident response phases, as follows:

| NIST 4 Phases | Activities |
|---|---|
| **Phase One: Preparation** | Research, council-wide generic and specialist cyber-security staff training and education, stake-holder engagement, exercise & backup restoration recoveries, expert contractual 3rd party support arrangements.<br>*Note: This phase and all subsequent phases <u>must</u> train for and consider and undertake forensic protection of the incident ‘attack’ evidence and response activity and decision log recording to facilitate criminal investigation/ prosecution and post-incident learning and improvement.* |
| **Phase Two: Detection & Analysis** | Training, alerting and monitoring and warning systems (infrastructure and cybersecurity) and IT Service Desk reporting through staff/ member diligence. |
| **Phase Three: Containment / Eradication and Recovery** | Subject to the type of attack and situational coordinated actions and response and recovery actions required. |
| **Phase Four: Post Incident Activity** | Debrief of staff/ consultants and learning outcomes reference any identified strengths and weaknesses of the situational response activities and outcome(s). |

The plan acknowledges and considers that the council has differing digital service continuity priorities at different times of the year (seasonality). For example, electoral digital service continuity has a very high priority approaching and during elections, or Emergency Planning digital services/ communications would be prioritised during an ongoing/ parallel running emergency planning response situation.

In this regard, the plan outlines early scenario engagement with the council's Chief Executive Officer - or his designated incident strategic lead (Gold Commander) - to agree prioritisation of digital service(s) recovery of one service over another, subject to;

a) The specific digital cyber-incident details being responded to and the nature and extent of services affected, and,

b) Due cognisance to any corresponding system architecture and digital service-related failure dependencies i.e. we need to have basic user-access supporting infrastructure working before we can recover an application else no users could access it.

Each of the four NIST phases and the council's arrangements are outlined, as follows.

## 4. PHASE ONE: PREPARATION

As initially outlined, this phase comprises officer and member stakeholder cyber awareness engagement and education. From an incident response preparatory perspective the council needs to maintain key training and is pro-active in doing so. Whilst this is an ongoing and evolving process within the council, preparatory actions will include the following:

| Stakeholder Engagement/ Training | Forum/ Audience | Approach/ Frequency |
|---|---|---|
| E-learning | Officers and Members | ▪ On induction.<br>▪ Periodically updated/ mandated to all. |
| Phishing awareness education and test campaigns | Officers and Members | ▪ Educational emails as the opportunity arises (e.g. a new NCSC or Local Government Association warning(s).<br>▪ Phishing campaigns 2-3 per annum. |
| Management Team cyber reports | Management Team and Audit Committee | ▪ Quarterly (alongside the Risk Management reporting regime).<br>▪ As urgency requires. |
| Senior Managers' Forum events | Senior Officers | Minimum of annually |
| All staff briefings | Officers | Minimum of bi-annually (every 2 years) in association with Essex Police Cyber-Crime Division. |
| All Member Briefings | Members | Minimum of annually |

| | | |
|---|---|---|
| Cyber Incident Planning and Response (CIPR) certificated training | Digital & Assurance Services Team - management | Minimum of two officers trained. |
| Certified Information Security Manager (CISM) certificated training | Digital & Assurance Services Team – Cyber-security | Minimum one officer trained. |
| Certified Information Systems Security Professional (CISSP) training | Digital & Assurance Services Team– Cyber-security | Minimum one officer to be trained. |
| Backup recovery/ viability exercising | Digital & Assurance Services Team – Technical Operations | Minimum monthly exercise. |
| CIRP Exercise (and/ or participation in ERF cyber exercises[s] ) | Digital & Assurance Services Team & key staff e.g. Communications Mngr | ▪ Minimum 6 monthly.<br>▪ Must include log-training |
| CIRP Document Review | Digital & Assurance Services Team | Annually. |

## 5. PHASE TWO: DETECTION & ANALYSIS

To maximise its cyber-defence monitoring and response capabilities the council has adopted a hybrid resourcing arrangement, comprising:

a) A specialist managed cyber-security contract (incumbent supplier Intergence Systems Ltd), providing:

- 24/7 alert monitoring, investigative services and incident support through the Intergence Systems Security Operations Centre (SOC).
- Specialist configuration, management and security patching of the council’s physical and cloud-based firewalls.
- Supply, support and management/ patching of a range of best-of-breed security monitoring and anti-malware products and services.
- Specialist consultancy and advice.

b) A small council in-house staff resource providing;

- An intelligent client and strategic support role.
- Specialist council support to services in its cyber-security and contract provisioning with third parties based upon a *security-through-design* new services ethos.
- Council-dedicated alert/ incident investigation monitoring and support.

The council’s specialist team play an active, registered engagement role with UK government National Cyber Security Centre (NCSC) briefings, guidance and compliance edicts and policies.

Similarly with the East of England Warning, Advice and Reporting Point (WARP) - a community-based service where members can receive and share up-to-date advice on information security threats, incidents and solutions. And with emerging Department of Levelling Up Housing and Communities (DLUHC) and Local Government Association guidance, briefings and new auditing regimes. The team plays a key advocacy role in the Essex Digital Partnership (EDP, previously EOLP) Cyber security group and including the Essex Resilience Forum (ERF) cyber response policy format, training/ exercising

The detection and analysis of a national or regional cyber-incident/ alert of successful cyber-breach could be cascaded downwards via NCSC, the WARP and/ or the ERF alerting process.

A Tendring District Council focussed attack or successful breach could be identified digitally through our alerting and monitoring systems or identified by a diligent member of staff.

In either event, both the in-house cyber-security and technical team and the contracted SOC play a key role in identifying and analysing the alert/ breach and escalating their assessment and recommended course of action to the Head of Service as quickly as can be achieved.

- **Vigilance, monitoring and alerting together with early and swift detection and situational analysis plays a crucial role in any cyber-attack successful response.**

## 6. PHASE THREE: CONTAINMENT, ERADICATION AND RECOVERY

Subject to the situational context and successful ‘breadth’ of infiltration and resultant outcome(s) and risks associated with the identified successful cyber-breach, the Digital Head of Service will assume the Tactical Commander/ Silver Commander role and engage with in-house service management team relevant experts - comprising the Cyber-security and Systems Manager, the Technical Operations Manager, the Information Governance and Services Manager, service-specific system sponsor manager (as appropriate) – together with expert consultancy resource available to resource and manage situation containment, eradication and recovery. The above mentioned officers will form the INITIAL core of the situation Tactical Coordination Group (TCG).

In the absence of the Digital Head of Service, the Cyber Security and Systems Manager will assume the incident lead tactical Silver Commander response role until any decision is taken by the newly-appointed situational Gold Commander to change/ revise this arrangement.

As a general ‘standing order’ principle BUT subject to <u>early</u> key corporate stakeholder engagement with the council’s Chief Executive or nominated Gold Officer, the cyber incident response will prioritise and recover services in descending priority order as follows;

### <u>FIRST: Corporate Operational Enabling Infrastructure, Risk To Life and Communications</u>

i. **Corporate Operational Supporting Infrastructure:** Functionally the minimum and basic requirements necessary to support and commence prioritised service recovery e.g. network access, remote working capabilities and WiFi (as appropriate).

ii. **Risk To Life Services:** Careline, consideration to other services subject to any parallel Emergency Planning operational incident response(s) e.g. a coastal flooding scenario.

iii. **Corporate Communication Channel(s)**: telephony, contact centre, website (informational services), Microsoft Office 365, mobile telephony, email.

## SECOND: Vulnerability And Minimal Staff Supporting Services

iv. **Vulnerable Persons Support Services**: Crematorium Services, Housing Benefits, Housing Services, Health & Safety.

v. **Officer Support and Member Local Democracy Resources:** Initial consideration to minimal officer system and democratic member system supporting requirements and events. For example Team Spirit HR system access or supporting an imminent scheduled Full Council Meeting.

## THIRD: Revenue Collection, Financial Accounting/ Payments

vi. **Revenue Collection/ Income And Financial Accounting Services**: Revenues Services (C/Tax, National Non-domestic rates), *MyTendring* self-service portal, card and payment services, Exchequer (payments), interactive website services.

## FOURTH: Statutory Services

vii. **Statutory Services:** Electoral Services, Waste and Recycling**,** Planning Services Environmental, Legal, Licensing, Enforcement, Emergency Planning.

## FIFTH: Income Generating Non-Statutory, Support And Governance And Non-Statutory (Other)

viii. **Income Generating Non-Statutory Services**: Leisure Centres, theatre, parking services.

ix. **Governance & Support Services:** Human Resources, Fraud, Risk Management, Internal Audit, Information Governance, Financial (non-revenue).

x. **Non-Statutory:** Other

## 7. Over –Arching Plan Approach And Behaviours

Unless the scenario is a 'business as usual' albeit significant digital fault response situation – which doesn't require invoking the CIRP - the council's digital service continuity and disaster recovery response will be delivered in accordance with adopted council Emergency Planning response 'best practice' arrangements with reference to this CIRP as a key process and procedural guide.

With cognisance to the need to respond decisively, quickly and flexibly and subject to the scenario encountered, the following trained and exercised roles and responsibilities will be adopted:

- Strategic Commander (Gold)
- Tactical Commander (Silver)

- Tactical Coordination Group (TCG) comprising relevant expertise of both staff and contractors.

Given the council's finite digital resources, members of the TCG may well directly undertake operational response duties and/or supervise operational staff to do so.

In the event of a multi-week or further protracted digital service continuity situational response the Gold Command, Silver Command and TCG responsibilities may be passed between different individuals subject to response continuity being maintained.

Alternatively, given the specialist digital skills and knowledge required from the incident 'Digital' Silver Commander and the 'Digital' TCG, early consideration should be given to reaching-out to the Essex Digital Partnership (EDP - previously the Essex Online Partnership) for mutual aid or shared responsibilities and resources if multiple organisations are affected.

All staff engaged in the situational response will;

- ✓ Maintain an up-to-date situational understanding at all times (or as per the latest briefing engagement between Gold and Silver Commanders).
- ✓ Work collaboratively and demonstrate commitment to resolving the service continuity issue(s), recovery and resolution.
- ✓ Communicate continuously and clearly.
- ✓ Be respectful of colleagues opinions and professional judgements and provide challenge in a supportive and empathic manner.
- ✓ Maintain a written log(s) of events, actions and decisions contemporaneously (at or around the time of).
- ✓ As appropriate and where necessary, establish an iterative/ evolutionary recovery scenario response aligned to business goals and objectives with applications and systems recovered in accordance with the application prioritisation/ dependency *appendix A embedded Excel Workbook* to this plan.
- ✓ Give due consideration to Agile Project Management MoSCoW prioritisation principles, namely;
    - ➢ **Must Have** applications and infrastructure - communication channels (telephony, email, contact centre), protective and vulnerable persons services e.g. Careline, Housing Benefits, MS Office,
    - ➢ **Should Have** applications – revenue collection and income management/ payment services, local government statutory functions, MyTendring self-service portal.
    - ➢ **Could Have** applications – non-statutory services or services where reasonable workarounds can be established in the short/ medium-term to deliver services.
    - ➢ **Won't Have** applications – where application recovery is delayed, or cannot be recovered or will not be recovered for some time these should be clearly documented and communicated clearly to the strategic command structure.

## 6.1 Duties And Responsibilities

Key incident duties/ responsibilities are as follows;

### 6.1.1 Strategic Commander (Gold)

This role is nominally the council's Chief Executive Officer (CEO) or his nominated incident Gold Commander(s). The Gold Commander will;

a) Liaise with the incident Tactical Commander (Silver) as early as can be achieved within the incident response timeline to confirm and agree clear strategic business goals/ service application recovery and continuity priorities and objectives.
b) Assume responsibility for member stakeholder communication(s), situational updates and engagement.
c) Liaise with the incident Tactical Commander (Silver) to agree the timing of periodic situational updates.
d) Maintain situational awareness and provide business strategic guidance.
e) May be called upon by the Tactical Commander to marshal and ensure that service System Sponsors / Application Asset Owners are fully engaging with the recovery and prioritising and resourcing their system testing responsibilities.

### 6.1.2 Tactical Commander (Silver)

This role is nominally the council's Head of Digital and Assurance Services or his nominated specialist incident Silver Commander(s) should the situation require mutual aid support. The Silver Commander will;

a) Adopt and enforce working to the NIST categories 2-4 - Detection and Analysis, Containment/ Eradication (As Appropriate), and Recovery/ repair and Post Incident Activity.
b) Establish a Tactical Coordination Group (TCG) comprising the relevant expertise(s) to effectively respond to the situation or event and resolve it – both in terms of technically and ongoing communication to stakeholders, customers and partners.
*c)* Establish a 'battle rhythm' and chair periodic TCG meetings (virtual or physical) that meets the pace of the evolving incident and TCG agreed actions. *Note: The Gold Commander situational update should ideally be timed to take place following these meeting(s).*
d) Liaise with the incident Strategic Commander (Gold) as early as can be achieved within the incident response timeline to;
    i. Explain the digital service continuity issue(s) and their resultant business continuity outcomes in a non-technical manner.
    ii. Discuss and agree any key strategic goals/ service application recovery and continuity priorities.
e) Ensure that any attack evidence is forensically protected/ safeguarded for potential use by future criminal investigation parties.
f) Ensure that the TCG and operational staff engaged in the incident commence and complete an event and decision log(s) of the incident.
g) Ensure that the Essex Resilience Framework (ERF) Cyber Incident Response Policy is followed in terms of communicating with partners and the National Cyber Security Centre (NCSC) and that policy escalation processes are adhered to.
h) Establish and maintain an awareness of the event/ situation and agree appropriate response(s), actions and lead and own the tactical response decision making process.

i) Engage with council's Emergency Planning Team to raise their awareness of the situation and to secure any relevant expert guidance.

j) Consider the need and establish rest periods and 'down time' for each facet of the TCG and operational supporting staff, together with the need to ask for additional mutual aid staffing resources – both from the Essex Digital Partnership and the National Cyber Security Centre (NCSC) or other third party specialist response organisations.

k) Lead and coordinate the TCG response to situational resolution in terms of: following strategy and guidance, compliance with council adopted policies and procedures/ plans, providing clear instructions and roles and responsibilities, any relevant contracts and contractual responses, partner and external body policies and engagement, response resourcing, health and safety.

l) Maintain situational awareness minute-to-minute, hour-to-hour and provide business response tactical guidance throughout the situation/ event.

m) In consultation with the Gold Commander, take ownership of declaring the end of each NIST phase and commencement of the next NIST phase in collaboration with the TCG specialists.

n) Lead and coordinate the TCG response until recovery/ resolution.

o) Organise the post-situational de-briefing.

### 6.1.3 Tactical Coordination Group (TCG)

Membership of the Tactical Coordination Group will be assigned by the Silver Commander based upon available skillsets, resources and the tactical response requirements.

Initially, the TCG is likely to comprise: digital expertise (staff and contractors), cybersecurity expertise, communication expertise, service application expertise. However, as the situation evolves additional expertise may be required or stood down, rested or replaced.

### 6.1.4 System Sponsors / Application Asset Owners

The System Sponsors / Application Asset Owners will play a key service continuity and disaster recovery response role in terms of coordinating expert system user resources to quickly test applications recovered, document any post-recovery issues and be fully engaged with the response/ recovery.

They will additionally play a key recovery TCG support role in terms of identifying, testing and communicating any necessary application workarounds.

### 6.1.5 Communications

Initial communications will be the responsibility of the Tactical Coordination Commander/ Silver Commander in consultation with the Gold Commander until such times as a communications expert(s) are engaged within the TCG group.

For the protection of the council's reputation all short-term communications will refer to *'technical difficulties'* and specifically not a cyber-attack. This includes all internal and external communications posted on the website or using social media with the explicit exception of communications between the Silver Commander and the Gold Commander, the management Team group and Cabinet.

The Gold Commander plays a key role in leading communications/ engaging with Members so that the Silver Commander and IT resources can focus on Detection Containment / Eradication and Recovery.

All external communication with partners will be in accordance with the adopted Essex Resilience Forum (ERF) cyber incident policy.

## 6.2 Wider Incident Response Planning And Situational Evolution Considerations

Subject to the specific incident response, the recovery longevity and wider council service business continuity effects the Gold Commander, in consultation with Silver Commander may wish to engage-with and empower the 'wider' council corporate Emergency Planning standing arrangements.

By doing so the Digital Head of Service Silver Commander may be replaced/ undertake and incident hand-over to a newly nominated, incoming 'corporate' Silver Commander - who in-turn will work with the council's Emergency Planning officers to form a new Tactical Co-ordination Group (TCG) with each of the relevant specialist cells.

In this scenario it is envisaged that the Digital Head of Service and/or the Cyber-security and Systems Manager (or their nominees) will assume the TCG role of Scientific and Technical Advisory Cell (STAC).

Corporate Emergency Planning plans and processes will take primacy in all things with the specific exception of the Digital Team working to delivering the NIST phases and operating in accordance with the ERF Cyber Security Reporting Policy.

## 6.3 Infrastructure And Application Restoration

The council's digital infrastructure is a complex hybrid blend of digital hardware supporting infrastructure comprising both on-premise private cloud supported applications (5%) together with public cloud supported applications and services (90%). The remaining 5% of applications are supported on private clouds under separate managed service agreements by third parties.

Given the above digital complexity, only a small amount of digital infrastructure and applications are delivered in isolation and without co-dependencies. The majority of council applications and services are reliant upon supporting infrastructure or have a range of application co-dependencies in-turn necessitating a strict order of service recovery/ re-instatement.

As outlined previously, adopting MoSCoW agile prioritisation and iterative recovery principles, and giving due consideration/ prioritisation to establishing base-line communications then vulnerable persons and protective services, then revenue collection and payment services, statutory services and finally non-statutory services the Appendix A Excel workbook (inserted below) provides an initial assessment guide for prioritised application recovery from which the TCG can work to with due cognisance to any Chief Executive/ Gold Commander business goal prioritisation guidance.

# 7 PHASE FOUR: POST INCIDENT ACTIVITY

The council's corporate Emergency Planning Team is well-versed in leading and undertaking post-incident reviews and documenting lessons learnt.

In this regard this CIRP proposes that the Emergency Planning Team are engaged to lead and deliver a cyber-attack post incident review meeting and resultant lessons learnt.

The Digital Head of Service will be responsible for ensuring that lessons learnt are incorporated into this CIRP document revision and adoption.

End