Corrective Action Plan – Security Risk Analysis 2021

Client Name: _____ Plan Start Date: _____

This form must be reviewed with members of the workforce who have the authority to implement required changes.

Prior to using this form - Entity should complete the TMC Security Risk Analysis (SRA). TMC recommends that the Entity work closely with their IT Partner to complete both the Risk Analysis and Corrective Action Plan. *Ensure all items identified in the SRA are addressed in the CAP.*

Instructions for using the Corrective Action Plan

1. In column one, list all items, vulnerabilities or *areas of weakness* that were identified with a circle on the Risk Analysis for the current year.
2. In column two, determine the type of threat(s) the weakness represents. *Refer to the lists below:*

THREATS

Human	**Natural**	**Technical**	**Environmental**	**Operational**
• Intentional harm by either worker or individual outside of the facility • Errors due to lack of concern or understanding of policy and procedure by worker	• Fire • Tornado • Flood • Hurricane	• Hardware or software failure • Malware • Use of new technologies	• Power failure • Temperature extremes • Chemical exposure • Liquid leaks	• Inadequate policies and procedures or lack thereof • Any process that affects the confidentiality, integrity, or availability of PHI.

3. In column three, determine the likelihood that the weakness (vulnerability) identified could impact the Organization.
4. In column four, determine the level of damage/access to protected health information if the organization is impacted.
5. In column five, outline the plan of action to eliminate or minimize the weakness (vulnerability).
   TMC recommends taking steps to eliminate or minimize all risks, regardless of level.
6. In column six, list who will be responsible for this plan of action and when the completion date is anticipated.

EXAMPLE

1. Vulnerability (Area of weakness identified in the Risk Analysis that must be addressed)	2. Type of Threat Represented (Check all that Apply)	3. Likelihood weakness will impact the organization Self-Assessment	4. Level of damage if impacted Self-Assessment	5. Plan of Action Our organization will either eliminate or minimize the vulnerability (weakness) in the following ways. *Additional Documentation Attached if needed	6. Responsible Party Time Frame for Completion Initial when project complete
No anti-virus protection for laptops	☐ Human ☐ Natural **X** Technical ☐ Environmental ☐ Operational	**X** High ☐ Medium ☐ Low	**X** High ☐ Medium ☐ Low	1. Review policies on purchase of new hardware. 2. Recall current inventory. 3. Install software to protect the mobile device.	IT Department 30 days
HIPAA training not provided for new hire employees	☐ Human ☐ Natural ☐ Technical ☐ Environmental **X** Operational	☐ High **X** Medium ☐ Low	☐ High **X** Medium ☐ Low	1. Identify all employees who have not been trained. 2. Provide instructions on access to TMC on-line training. 3. Allow adequate time to complete training modules. 4. Workers must pass posttest with 80% score.	Manager 30 days

CORRECTIVE ACTION PLAN 2021

1. Vulnerability (Area of weakness outlined in the Risk Analysis)	2. Type of Threat Represented (Check all that Apply)	3. Likelihood weakness will impact the organization Self-Assessment	4. Level of damage if impacted Self-Assessment	5. Plan of Action Our organization will either eliminate or minimize the vulnerability (weakness) in the following ways. *Additional Documentation Attached if needed	6. Responsible Party Time Frame for Completion Initial when project complete
Areas addressed on CAP from previous year. ☐ YES ☐ NO		☐ High ☐ Medium ☐ Low	☐ High ☐ Medium ☐ Low	If no, corrections for areas of vulnerability should be addressed on the CAP from the previous year.	
	☐ Human ☐ Natural ☐ Technical ☐ Environmental ☐ Operational	☐ High ☐ Medium ☐ Low	☐ High ☐ Medium ☐ Low		
	☐ Human ☐ Natural ☐ Technical ☐ Environmental ☐ Operational	☐ High ☐ Medium ☐ Low	☐ High ☐ Medium ☐ Low		
	☐ Human ☐ Natural ☐ Technical ☐ Environmental ☐ Operational	☐ High ☐ Medium ☐ Low	☐ High ☐ Medium ☐ Low		

1. Vulnerability (Area of weakness outlined in the Risk Analysis)	2. Type of Threat Represented (Check all that Apply)	3. Likelihood weakness will impact the organization Self-Assessment	4. Level of damage if impacted Self-Assessment	5. Plan of Action Our organization will either eliminate or minimize the vulnerability (weakness) in the following ways. *Additional Documentation Attached if needed	6. Responsible Party Time Frame for Completion Initial when project complete
	☐ Human ☐ Natural ☐ Technical ☐ Environmental ☐ Operational	☐ High ☐ Medium ☐ Low	☐ High ☐ Medium ☐ Low		
	☐ Human ☐ Natural ☐ Technical ☐ Environmental ☐ Operational	☐ High ☐ Medium ☐ Low	☐ High ☐ Medium ☐ Low		
	☐ Human ☐ Natural ☐ Technical ☐ Environmental ☐ Operational	☐ High ☐ Medium ☐ Low	☐ High ☐ Medium ☐ Low		
	☐ Human ☐ Natural ☐ Technical ☐ Environmental ☐ Operational	☐ High ☐ Medium ☐ Low	☐ High ☐ Medium ☐ Low		

1. Vulnerability (Area of weakness outlined in the Risk Analysis)	2. Type of Threat Represented (Check all that Apply)	3. Likelihood weakness will impact the organization Self-Assessment	4. Level of damage if impacted Self-Assessment	5. Plan of Action Our organization will either eliminate or minimize the vulnerability (weakness) in the following ways. *Additional Documentation Attached if needed	6. Responsible Party / Time Frame for Completion / Initial when project complete
	☐ Human ☐ Natural ☐ Technical ☐ Environmental ☐ Operational	☐ High ☐ Medium ☐ Low	☐ High ☐ Medium ☐ Low		
	☐ Human ☐ Natural ☐ Technical ☐ Environmental ☐ Operational	☐ High ☐ Medium ☐ Low	☐ High ☐ Medium ☐ Low		
	☐ Human ☐ Natural ☐ Technical ☐ Environmental ☐ Operational	☐ High ☐ Medium ☐ Low	☐ High ☐ Medium ☐ Low		
	☐ Human ☐ Natural ☐ Technical ☐ Environmental ☐ Operational	☐ High ☐ Medium ☐ Low	☐ High ☐ Medium ☐ Low		

1. Vulnerability (Area of weakness outlined in the Risk Analysis)	2. Type of Threat Represented (Check all that Apply)	3. Likelihood weakness will impact the organization Self-Assessment	4. Level of damage if impacted Self-Assessment	5. Plan of Action Our organization will either eliminate or minimize the vulnerability (weakness) in the following ways. *Additional Documentation Attached if needed	6. Responsible Party Time Frame for Completion Initial when project complete
	☐ Human ☐ Natural ☐ Technical ☐ Environmental ☐ Operational	☐ High ☐ Medium ☐ Low	☐ High ☐ Medium ☐ Low		
	☐ Human ☐ Natural ☐ Technical ☐ Environmental ☐ Operational	☐ High ☐ Medium ☐ Low	☐ High ☐ Medium ☐ Low		

The CAP was completed by the Privacy/Security Officer or other authorized member of management, and the results of both the Security Risk Analysis and CAP have been reviewed with the leadership team of the Covered Entity, and the workforce, as appropriate.

_____
Privacy Officer Date

_____
Security Officer Date

_____
IT Manager/Group Date

_____
Administrator/Manager Date

_____
CEO/Owner Date